International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.011 ISSN: 2581-4621

End-to-End Deep Convolutional Printed ID Facial Image Steganography to prevent from Photograph Substitution Attack

A Ranjith
Department of ECE
Muthayammal Engineering College,
Namakkal,India.
aranjithofficial@gmail.com

P Tharun
Department of ECE
Muthayammal Engineering College,
Namakkal,India.
ruthintharun1202@gmail.com

R Tharun Sriram
Department of ECE
Muthayammal Engineering College,
Namakkal,India
tharunsriram.r@gmail.com

S Selvarasu
Department of ECE
Muthayammal Engineering College,
Namakkal,India.
selvarasumec@gmail.com

ABSTRACT
At the point when we discuss "character card," we're alluding to an official picture ID that can be utilized as such at least in Germany. Shrewd to travel archives, electronic IDs, electronic marks, civil cards, key cards for getting to safeguarded regions or organization framework, government backed retirement cards, and so on are only a portion of the furthermost common purposes for brilliant cards. There are a measure of shields included into these records. Battle the act of report distortion. Criminal assaults against character confirmation frameworks right now depend on wrongfully acquiring genuine archives and adjusting facial pictures in light of the fact that these security components are hard to overcome. Having an arrangement of believed characters is critical to any useful society. These state run administrations and personality producers ought to consistently refresh and improve their security conventions to decrease the probability of extortion. Thus, we convey StegoCard, the principal pragmatic steganography approach customized explicitly for photographs regularly found on standard ID cards. StegoCard is a full-stack facial picture steganography model that utilizes a Profound Convolutional Auto Encoder to make a representation of a Stego that disguises a message and a Profound Convolutional Auto Decoder to decipher the picture. Capable is the decoder. The Stego picture fills in as a message decoder. This turns out as expected regardless of whether the picture was printed out and subsequently digitized. Examinations of He Stego Stamp and StegoCard encoded face photos show that the last option are of higher perceptual quality. Top motion toward clamor proportion, disguising power, and quietness scores on the test set are utilized as show measurements.
Keywords : Convolutional Auto Encoder, Convolutional Auto Decoder steganography, StegoCard,

I.INTRODUCTION

A. Overview

As things stand, encoding a message inside a picture or message allows for the possibility of sending a message that is visible to both the transporter and the typical recipient. Steganography suggests that information can be covertly hidden and then made visible when needed. The proverb "cover picture" suggests a fake picture, however the maxim "stego-picture" suggests the real picture after it has been hidden. Cryptography encrypts a secret message to prevent eavesdroppers from deciphering it. Combining encryption and steganography provides an additional layer of security in this way. Picture pressure allowed us to reduce the message's archive size while increasing its mystery.

Steganography is a common type of encryption where a picture is used to conceal a secret message. Modern photos are sometimes employed as cover objects because of their widespread online presence. This is because they provide an ample amount of pixel abundance that may be utilized to conceal limited

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.011 ISSN: 2581-4621

information without detracting from the overall aesthetic of the image. Starting with the technique for hiding data in the least basic portions of the image (LSBs)

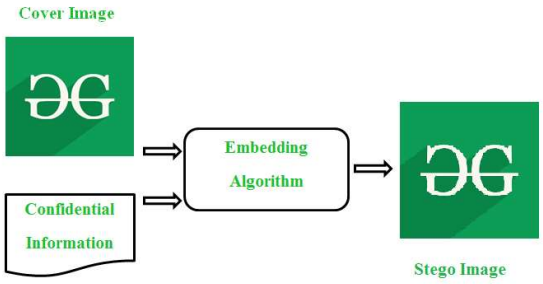
The field of picture steganography has advanced to more intricate techniques such as material flexible steganography, wherein a mutilation capacity is used to efficiently modify embedding costs to each cover pixel. Restricting a twisting capacity is how cover picture introduction is accomplished. In order to increase the security of covert dispatches in an open structure scenario, it is essential to conceal the dispatch's actual state and current state from unauthorized beneficiaries. The "investigation of hidden or secret correspondence" is the term for it.

Any steganographic method must meet the three requirements of cutoff, straightforwardness, and generosity in order to be deemed successful. The most sensitive information that can be handled within a record is its limitation. The steganographic technique is completely safe and intangible if the data on the cover and the stego records are almost identical. In summary, the Stego report should provide strong points; it can withstand several attacks and still reveal the hidden message with minimal information loss.

B.STEGNOGRAPHY

The technique of hiding information within a different message or tangible object to evade discovery is known as steganography. Almost any kind of digital content, including text, images, videos, and audio, can be concealed via steganography. At its destination, the concealed data is subsequently revealed.Sometimes, data that is hidden using steganography is encrypted before being hidden in a different type of file. It might be treated in some way to make it more difficult to find if it isn't encrypted.

Steganography is sometimes likened to cryptography as a means of secret communication. But the two are not the same since steganography does not require data to be encrypted before transmission or decrypted after receipt using a key.



II.RELATED WORKS

Lianqiang Niu,et al,[1], Existing image steganography technology can resist image attacks, however, the quality of generated encoded image is poor and the low-frequency region can be perceived. To improve the quality of the encoded image, an image steganography method based on texture analysis is proposed. In this method, the gray-level co-occurrence matrix is used to extract the texture information of the cover image, the information is embedded in the complex position of the image, in and the network structure of the StegaStamp encoder is improved, small convolution layers are added in the down-sampling process to expand the receptive field, and channel attention is used to assign different weights to feature channels to enhance the influence of important features of images. The experimental results show that the proposed method can effectively improve the PSNR and SSIM values of coded image, and the quality is improved without degrading the robustness and embedding capacity.

Sowmya K. S,et al,[2], This research paper explores the use of image steganography for data communication. It provides an overview of data communication and steganography and focuses on the specific area of image steganography. It surveys various algorithms, including traditional and recent techniques, such as least significant bit insertion and neural network-based approaches. The importance of security implementation and recent advancements in deep learning techniques, such as GANs and CNNs, are also discussed. The paper concludes with a discussion of future directions and open challenges in the field of image steganography for data communication.

A. Geetha Devi,et al,[5], Steganography is a means of secretly concealing information in which the act of steganography itself is hidden in plain sight. Steganography is also known as “stealth writing.” Steganography is not a suitable replacement for cryptography; nevertheless, it can be used in conjunction with cryptography to further strengthen the information hiding mechanism. Steganography is not a good

DOI:10.46647/ijetms.2025.v09i02.011 ISSN: 2581-4621

replacement for cryptography. The cover media for a steganographic method can be anything that can be represented digitally, such as a text file, image, audio file, video file, Transmission Control Protocol/Internet Protocol packet, or any other entity. Steganography can be used to hide information in these and other formats. First, the Robust Multitier Spatial Domain Secured Color Image Steganography in Server Environment (MSS-SE) approach is created as part of an effort to lower the possibility of compromising confidential communications. MSS-SE steganography methods, rather than transmitting the original picture from the server, send a randomized mix of a cover image and a confused image from the same server. This is done in place of delivering the original image. A unique approach that is based on deep hierarchical spectral spatial feature fusion has been developed by us in order to improve the classification of HSIs (DHSSFF). The pooling method, which is considered by CNN to be one of the most important regularization procedures, has been the primary focus of our attention prior to the construction of the model. Following an examination of the relevant published material, we have reached the conclusion that a wide variety of pooling algorithms have been applied to carry out fruitful analyses of remote sensing data.

Kholood Ayed Almalkil,et al,[7Hiding confidential digital information in today's modern communication system is a very challenging task. Even though many algorithms have been developed to ensure the security of information delivered via the communication channel, many flaws have been discovered over time. Steganography is the science of hiding the existence of secret information. The concept of steganography is about embedding the secret data in a cover file in which the cover file could be an image, audio, video, text, or any other medium. Successfully formulating an algorithm that embeds the secret information in a cover file will produce a new file called the stego file. This research aims to develop a new methodology in which the secret information will be embedded into a legitimate URL link. Unlike the usual methods that hide the secret message in the content of another file, this method uses a valid form of the URL link to hide the secret message. Since the URL is a type of text that links users to a web page and is not an informative text to be read, it results in a secure method to pass secret information as no one pays attention to a URL text. This method combines and implements different techniques, abbreviates, searches, and matches bits and converts to allowed URL characters to encode the secret message. The results show that it works well with legitimate URLs, including the website's homepage URL.

Jingyi Qiu,et al,[8], The popularity of the Internet and the development of multimedia technology have made it easier to store, modify, and share digital multimedia information (text, audio, video, etc). Because multimedia data contains some personal information, if this information is intercepted and stolen by an illegal third party, resulting in the public transmission of the information on the Internet, then the personal contact between the communicating parties will no longer be private. Therefore, how to ensure communication privacy and information security has always been an important issue that is difficult to get rid of in the development of the Internet. This paper studies the generative image steganography scheme based on deep learning, understands the related theories of image steganography and deep learning based on the literature, and then designs the generative image steganography scheme based on deep learning, and the designed scheme is tested, and the test results show that the steganography scheme designed in this paper has better performance in accuracy. Compared with the traditional scheme, the difference between the two is up to 4%.

III.METHODOLOGY

A. Existing System

Watermarks are patterns applied to the ID card during the manufacturing process that can be viewed or unseen. Watermarks make playing cards more difficult to copy since they can be uniquely shaped and only visible when handled in a specific manner. Microtext is incredibly small textual content that appears on cardboard in certain places.

If people don't know how to look for it, it's extremely difficult to replicate.

ID playing cards have a holographic lamination that adds another level of obvious security. Holographic laminate is used on driver's licenses so that people can easily determine whether or not the license is still valid. Not only is it difficult to replicate holographic laminate since the right computer is required, but the layout of the laminate is specially created as well.

preserving homes and campuses steady as get admission to to distinctive regions is limited for the ones with out the right ID card. Using magnetic stripes, you may additionally designate distinctive stages of safety clearance for distinctive card holders so that they've get admission to to the right places. Barcodes also are

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.011 ISSN: 2581-4621

brilliant for fast and without difficulty figuring out ID playing cards as valid for your ID card machine or now no longer.

Biometric statistics may be the most reliable security feature you may have for your ID playing cards. This data verifies that the cardboard holder is who they claim to be by looking at layers, layout, and integrated technology. While photo ID playing cards can significantly reduce safety risks, both human look and snapshots may be modified. It is possible to verify that the ID card truly belongs to the cardholder by using fingerprints and virtual signatures covered on the card.

B. Proposed System

The system that is planned is called StegoFace. Using pictures of people's faces, StegoFace is an ID and MRTD-relevant model for encoding and decoding clandestine communications. Being the first model to be industrialized specifically as a document security strategy, we are extremely proud of our model. verification of a portrait. with the application of a steganographic image. StegoFace consists of the following two steps: input/output devices (encoder/decoder).

Recurrent Proposal Network (RPN)

Object boundaries and non-object scores can be predicted at each location using a Region (RPN), which is a fully To guarantee that it recommends dependable places, the RPN undergoes regular training. In order to anticipate regional suggestions spanning scales and aspect ratios, RPN was developed. RPN uses an adjustable anchor box as a point of reference that may be changed and redesigned to accommodate different screen sizes. This method can be considered a pyramid of recursive references, as it avoids listing images or filters with multiple scales or aspect ratios.

The algorithm for Binary Error-Correcting Codes A Binary Error-Correcting Codes technique is used to convert a secret message into a binary message during encoding. The secret message is extracted from the binary transmission at the decoding stage using the same Binary Error-Correcting Code approach.

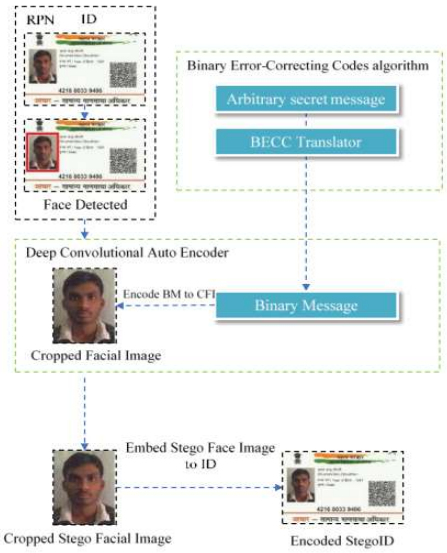
Deep Convolutional Auto Encoder

The generator's initial phase consists of the encoder network. Maximizing the perceptual accuracy with which the input image may be reconstructed should be the goal of an encoder's training. The ability of a decoder to uncover information that is encoded. An image of a face and a coded message are provided to the encoder as initial input. The encoder application's last step is to utilize the pre-trained encoder perfect to embed the message into the cropped face in order to make the encoded face image. The original face image is not printed on ID cards; instead, an encoded cropped image is used to avoid identity theft.

Deep Convolutional Auto Decoder

Secret messages can be sent and received using face photographs, and decoders are designed to decode

C. Proposed Block Diagram



International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.011 ISSN: 2581-4621

Auto Encoder

The encoder community is the first component of the generator. The goal of the encoder education process is to maximize the trade-off between the decoder's overall effectiveness in extracting the secret message and its capacity to fix the entry images' perceptual properties. We chose an encoder community structure that is generally based entirely on UNets; yet, the In order to preserve the statistics of the game messages that would otherwise be lost over community education, pooling layers have been removed.

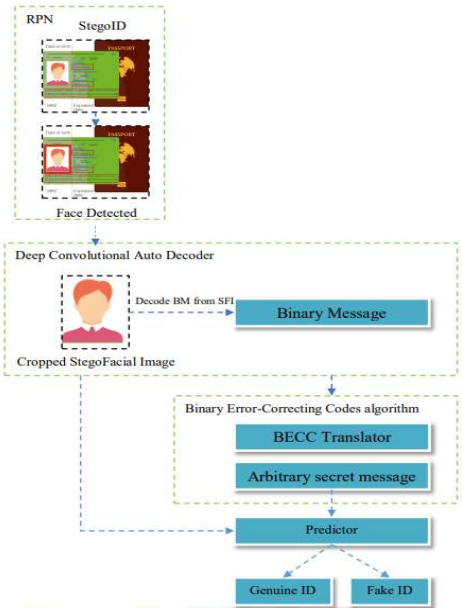
Both the preprocessing module and the embedding community as a whole are mostly built around the idea of an auto-encoder structure. The preprocessing module and the embedding community form an hourglass shape with expanding and contracting sections. The community of autoencoders examines the input and extracts the features that can be used to the component of encoding. The function depiction of the enter is the latent region in an autoencoder. The output photograph is reconstructed from the latent area using the decoder, a component of the autoencoder. Programs for image steganography no longer require dimensionality adjustments; instead, the latent area has to contain the name of the game photograph and the quilt photograph's mixed function illustration.

The preprocessing module's concatenation capabilities are used by the embedding community to create a latent area and reconstruct the stegoface—which closely resembles the quilt photograph—from the latent area. Each discrete portion of the quilt photograph contains a piece of the game photograph's name buried therein. The Convolutional layers with an increasing number of filters are used in the design of embedding communities. The name of the game photograph concatenated with each cowl photograph's finer capabilities is represented by the latent area on the encoder's cease.

Auto Decoder

The community of decoders After applying the noise to the images, this is included into the overall framework. The goal of the decoder is to decipher a message that is encoded in a face photo. RPN makes it possible for this community to crop off the appropriate area and equalize its scale, which can make the task of deciphering the steganography easier to do and improve performance all around. The method eliminates spatial invariance from the encoded pictures by utilizing a learnable affine transformation in conjunction with interpolation.

The DCAD is positioned later than the RPN block. The objective of the extraction community is to extract the game photo's name that is concealed inside the stego image. After conducting controlled testing, it seems that a structure similar to the embedding community offers the best results for obtaining the game photo's name with the least amount of data loss. The community of extractives includes a segment that increases and a piece that contracts. The range of filters, cutoff size, step, and other hyperparameters are adjusted mostly depending on the results of the experiments. The structure that yielded the excellent outcome is described here.



DOI:10.46647/ijetms.2025.v09i02.011 ISSN: 2581-4621

VI. RESULT ANALYSIS

This web program makes it easy for organizations to verify their employees' identity documents remotely by utilizing a number of cutting-edge technologies. This technique has the ability to solve the widespread issue of national identity card manipulation and falsification.

V.CONCLUSION

The main goal of this white paper is to conceal the information that is security-encoded in ID and MRTD documents while maintaining the ability to verify the integrity of the portrait. In light of this, we provide StegoFace, the first workable steganography solution designed especially for the face photographs commonly found on IDs and MRTDs. Using a deep convolutional autoencoder to produce encoded images with hidden secret messages in face portraits and a deep convolutional autodecoder to interpret those messages, StegoFace is a full-stack neural network. rise. The message is still an encoded image even if the image was printed and then scanned. StegoFace is superior to existing methods because it allows images to be used in their original contexts, regardless of where they were taken.

FUTURE WORK

In order to preserve identities and prevent them from being easily recognized, the scope of a machine to find and code faces in ID photos is suggested in this project. In addition to using steganography and a novel, robust, and potent encoding machine, the device recognizes faces. The innovative device uses a key region that can be multiplied depending on safety measures so that one can be used. It also has excellent defenses against specific types of attacks, such as picturegraph replacement attack.

VI.REFERENCES

1. Ferreira, E. Nowroozi, and M. Barni, ‘‘VIPPrint: Validating artificial photograph detection and supply linking techniques on a large-scale dataset of published documents,’’ J. Imag., vol. 7, no. 3, p. 50, Mar. 2021.
2. Bazarevsky, Y. Kartynnik, A. Vakunov, K. Raveendran, and M. Grundmann, ‘‘BlazeFace: Sub-millisecond neural face detection on cellular GPUs,’’ 2019, arXiv:1907.05047.
3. .J. Deng, J. Guo, N. Xue, and S. Zafeiriou, ‘‘ArcFace: Additive angular margin loss for deep face recognition,’’ in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2019, pp. 4685–4694
4. R. L. Jones, Y. Wu, D. Bi, and R. A. Eckel, ‘‘Line phase code for embedding information,’’ U.S. Patent App. sixteen 236 969, Jul. 4, 2019.
5. S. Ciftci, A. O. Akyuz, and T. Ebrahimi, “A Reliable and Reversible Image Privacy Protection Based on False Colors,” IEEE Transactions on Multimedia, vol. 20, no. 1, pp. 68–81, 2018.

6. M. Jiménez Rodríguez, C. E. Padilla Leyferman, J. C. Estrada Gutiérrez, M. G. González Novoa, H. Gómez Rodríguez, and O. Flores Siordia, “Steganography implemented withinside the beginning declare of images captured with the aid of using drones primarily based totally on chaos,” Ingeniería e Investigación, vol. 38, no. 2, pp. 61–69, 2018.
7. L.-C. Chen, G. Papandreou, I. Kokkinos, K. Murphy, and A. L. Yuille, ‘‘DeepLab: Semantic photograph segmentation with deep convolutional nets, atrous convolution, and completely related CRFs,’’ IEEE Trans. Pattern Anal. Mach. Intell., vol. 40, no. 4, pp. 834–848, Apr. 2018.
8. Ü. Çavusoglu, S. Kaçar, I. Pehlivan, and A. Zengin, “Secure photograph encryption set of rules layout the use of a unique chaos-primarily based totally S-Box,” Chaos, Solitons & Fractals, vol. 95, pp. 92–101, 2017.
9. Z. Parvin, H. Seyedarabi, and M. Shamsi, “A new steady and touchy photograph encryption scheme primarily based totally on new substitution with chaotic function,” Multimedia Tools and Applications, vol. 75, no. 17, pp. 10631–10648, 2016.
10. M. Khan and T. Shah, “An green chaotic photograph encryption scheme,” Neural Computing and Applications, vol. 26, no. 5, pp. 1137–1148, 2015